



SPYWOLF

Security Audit Report



Completed on
December 3, 2022

MADE IN USA 

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **Ryz3 - Messi** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



Ryz3



PROJECT DESCRIPTION

According to their website:

The first Binary Tokens powering web3 speculation – think online betting merged with defi investing.

“Messi v Ronaldo: Top Goal Scorer” is the first official Ryz3 event – an alpha launch of the first Binary Tokens. Players can participate by purchasing either the Messi or Ronaldo token from PancakeSwap. A percentage of all transactions will be added to a prize pool that gets distributed as BUSD to the holders of the current winning token, that is the current Top Goal Scorer + Assists in the 2022 FIFA World Cup between Lionel Messi and Cristiano Ronaldo. At regular intervals, the leader is determined externally by a data feed provider. In Layman’s terms, if you’re holding Messi token, and Messi is currently leading the goals and assists, then you earn bonus BUSD just for holding!

Release Date: Presale starts in December 3, 2022

Category: Betting

01





CONTRACT INFO

Token Name Ryz3 Messi	Symbol RZMESSI
Contract Address 0x3bc84253CD67fbe7b9ffD1F7b7185A39B38DD445	
Network Binance Smart Chain	Language Solidity
Deployment Date Dec 03, 2022	Verified? Yes
Total Supply 1,000,000,000	Status Not launched

TAXES



*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of Dec 3, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
No limit

DEX:
PancakeSwap

LP Address(es)

Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	1902000000 RZMESSI
Median Transfer Amount	1000000000 RZMESSI
Average Transfer Amount	951000000 RZMESSI
First transfer date	2022-12-03
Last transfer date	2022-12-03
Days token transferred	1

SMART CONTRACT STATS

Calls Count	14
External calls	1
Internal calls	13
Transactions count	5
Uniq Callers	3
Days contract called	1
Last transaction time	2022-12-03 06:52:31 UTC
Created	2022-12-03 06:04:53 UTC
Create TX	0xa9afc373a79f1db85c312417d5b0dd0d10a661f5cba678176138f49ae4e5cbce
Creator	0x05b5e42d405fbf5fc427f5caf1f7fac571a90399

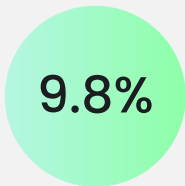


FEATURED WALLETS

Owner address	0x05b5e42d405fbf5fc427f5caf1f7fac571a90399
Marketing fee receiver	0x498af46b48706449b6e66edfd2c85befa4a500da
Community fee receiver	Same as Marketing receiver
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS

1



9.8%

0xbee494a8fac9c6927631c2335977f8c06c8e4572



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

Medium Risk

Owner can set buy/sell fees up to 25%.
Combined buy+sell=50%.

```
function setAllBuyFees (
    uint256 allReward,
    uint256 allmarketingDev,
    uint256 allliquidity,
    uint256 allCommunity,
    uint256 allBurn
) public onlyOwner {
    buyTotalFees = allReward.add(allmarketingDev).add(allliquidity).add(allCommunity).add(allBurn);
    require(buyTotalFees <= 25, "Total Fee must be less than 25%");

    binaryA.updateBuyFees(allReward, allmarketingDev, allliquidity, allCommunity, allBurn);
    binaryB.updateBuyFees(allReward, allmarketingDev, allliquidity, allCommunity, allBurn);
}

function setAllSellFees (
    uint256 allReward,
    uint256 allmarketingDev,
    uint256 allliquidity,
    uint256 allCommunity,
    uint256 allBurn
) public onlyOwner {
    sellTotalFees = allReward.add(allmarketingDev).add(allliquidity).add(allCommunity).add(allBurn);
    require(sellTotalFees <= 25, "Total Fee must be less than 25%");

    binaryA.updateSellFees(allReward, allmarketingDev, allliquidity, allCommunity, allBurn);
    binaryB.updateSellFees(allReward, allmarketingDev, allliquidity, allCommunity, allBurn);
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



Informational

Owner can withdraw thee rewards accumulated in dividend distributor contract.

```
function purgeBeforeSwitch() public onlyParentOwner {
    dividendDistributorSelf.purge(msg.sender);
}

function purge(address receiver) external override onlyControllerOrToken {
    uint256 balance = REWARD.balanceOf(address(this));
    REWARD.transfer(receiver, balance);
}
```

Owner can set score controller.

Score controler can change scores for each binary token contract.

```
function setScoreController(address controller) public onlyOwner {
    _scoreController = controller;
    emit ScoreControllerUpdated(controller);
}

function updateScores(uint256 scoreA, uint256 scoreB) public onlyScoreController {
    require(scoreA >= 0 && scoreB >= 0);
    binaryA_Score = scoreA;
    binaryB_Score = scoreB;
    emit ScoresChanged(scoreA, scoreB);
}
```



Informational

Owner can exclude address from fees and dividends.

```
function setIsDividendExemptForAll(address holder, bool exempt) public onlyOwner {
    binaryA.setIsDividendExempt(holder, exempt);
    binaryB.setIsDividendExempt(holder, exempt);
}

function setIsFeeExemptForAll(address holder, bool exempt) public onlyOwner {
    binaryA.setIsFeeExempt(holder, exempt);
    binaryB.setIsFeeExempt(holder, exempt);
}

function setIsDividendExempt(address holder, bool exempt)
    external
    onlyParentOwner
{
    require(holder != address(this) && holder != pair);
    isDividendExempt[holder] = exempt;
    if (exempt) {
        dividendDistributorSelf.setShare(holder, 0);
    } else {
        dividendDistributorSelf.setShare(holder, _balances[holder]);
    }
}

function setIsFeeExempt(address holder, bool exempt) external onlyParentOwner {
    isFeeExempt[holder] = exempt;
}
```



Informational

Owner can set rewards distribution criteria (period and min rewards to be distributed).

```
function setDistributionCriteria(
    uint256 _minPeriod,
    uint256 _minDistribution
) external onlyParentOwner {
    dividendDistributorSelf.setDistributionCriteria(
        _minPeriod,
        _minDistribution
    );
}
```

Owner can withdraw bnb from the contract.

```
function clearStuckBalance(uint256 amountPercentage) external onlyParentOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer((amountBNB * amountPercentage) / 100);
}
```

Owner can change the reward token.

```
function changeSwapToken(address token) external onlyParentOwner {
    SWAPTOKEN = token;
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Ryz3 Messi

GOOD PRACTICES FOUND

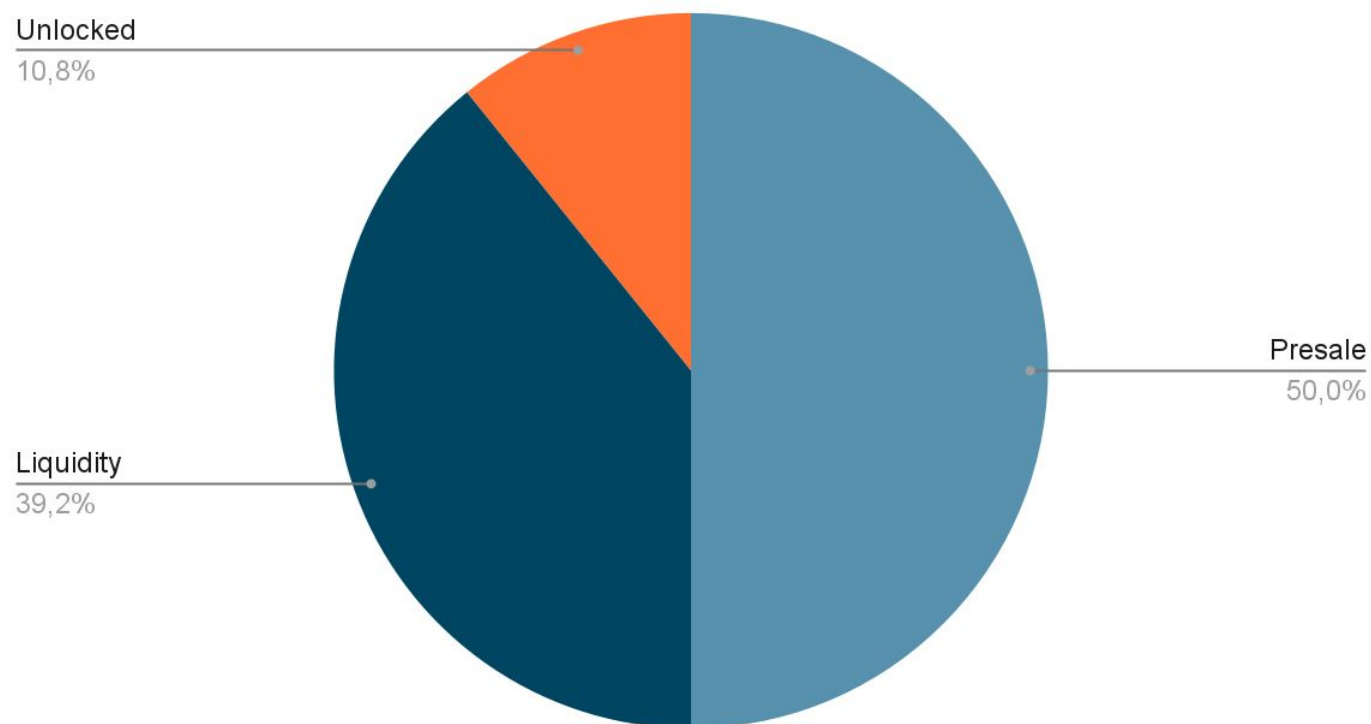
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



Initial tokens distribution according to Pinksale's presale page:

- 50% - Presale
- 10.8% - Unlocked
- 39.2% - Liquidity

Tokens distribution



TOKENOMICS



THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://ryz3.com/>

Domain Registry

Expires on 2023-08-12

Domain Expiration

May 3, 2025

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Single page design, appropriate color scheme and graphics.

Content

The information can be more explanatory to help new investors understand what the product does right away. No grammar mistakes found.

Whitepaper

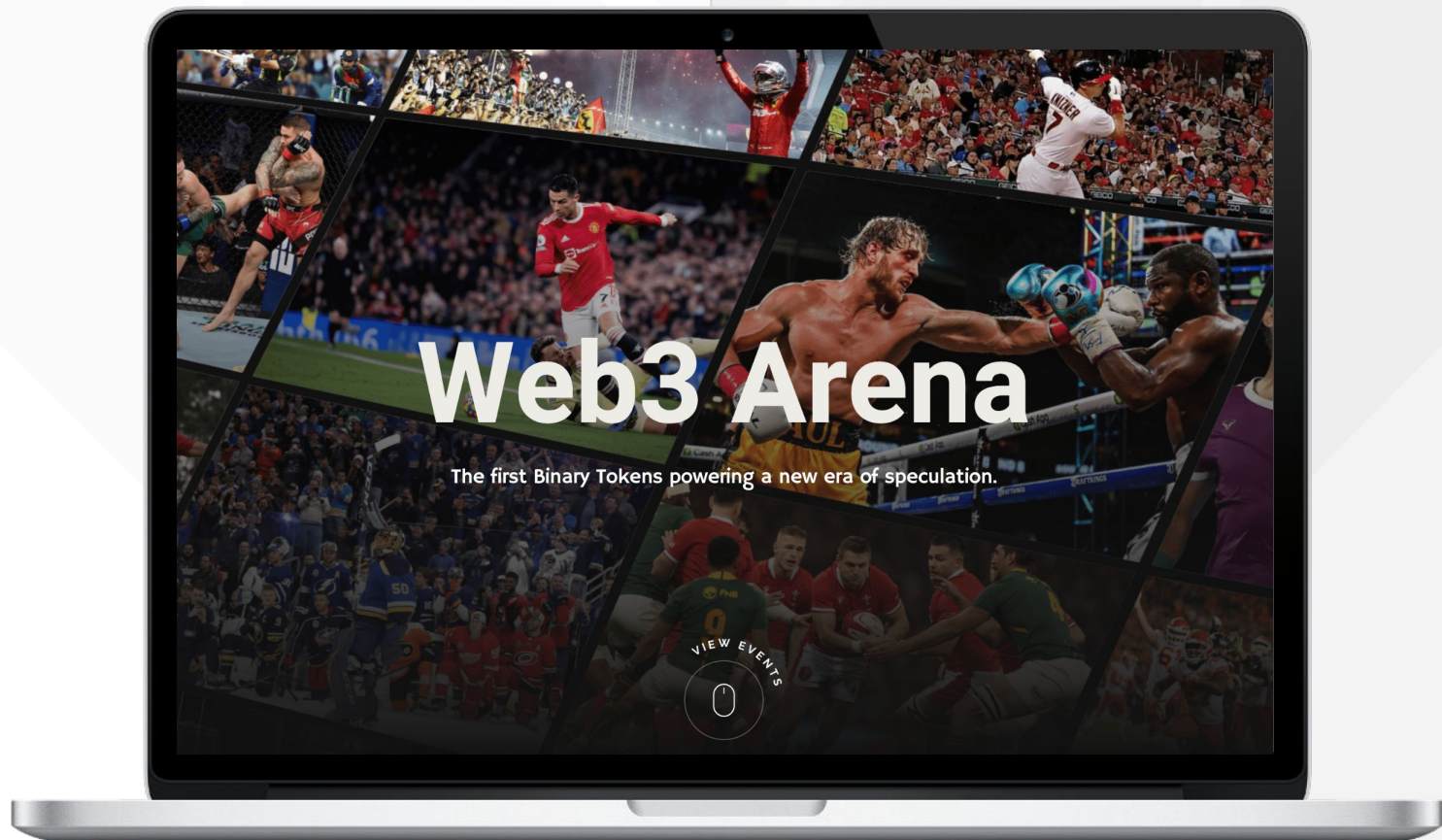
⚠ No whitepaper.

Roadmap

⚠ No roadmap.

Mobile-friendly?

Yes



ryz3.com

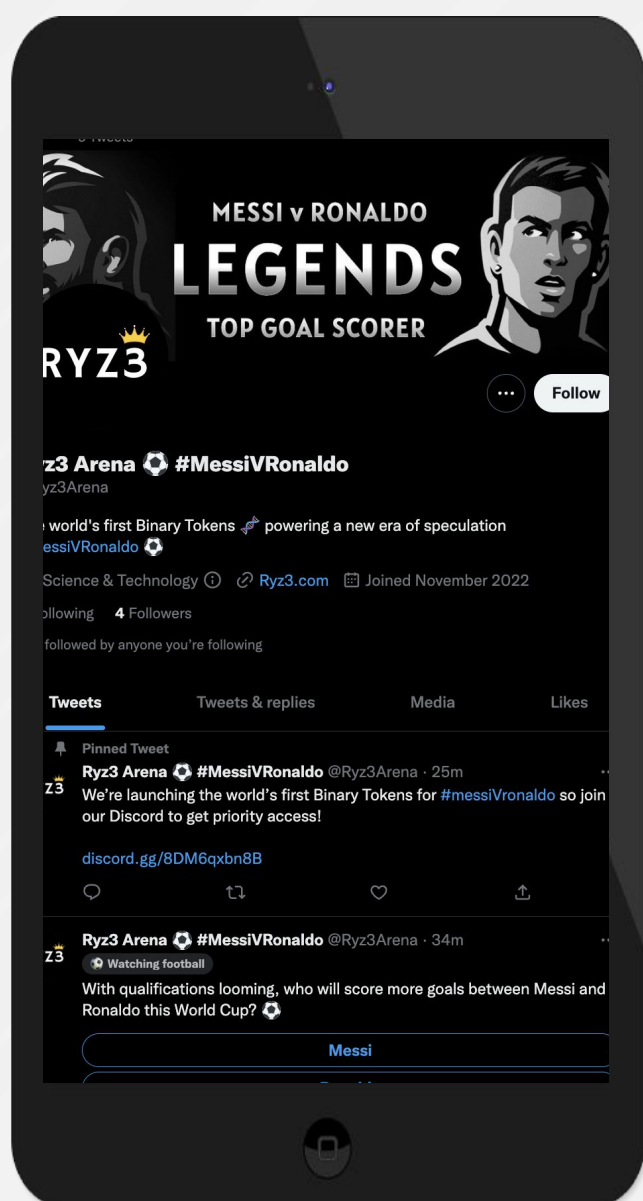


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

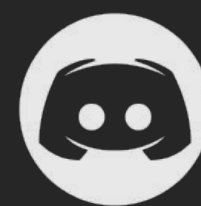
Project's social media activity is concentrated mainly in Discord and consists of active members



Twitter

@Ryz3Arena

- 10 followers ⚠️
- Active, posts frequently



Discord

<https://discord.com/invite/8DM6qxbn8B>

- 122 Members
- 100 Online members



Telegram

- Not available



Medium

Medium link here

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[SPYWOLF.NETWORK](https://spywolf.network)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFOFFICIAL](https://t.me/SPYWOLFOFFICIAL)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://github.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.